C12 Data Decryption of Android™ Third-Party Private Messaging Apps: A Case Study

Lyndsay Haak, BS*, Marshall University Forensic Science Center, Huntington, WV 25701; Josh Brunty, MS*, Marshall University, Huntington, WV 25701

Learning Overview: After attending this presentation, attendees will understand how the app CoverMe operates and how messages sent through the app are decrypted. This presentation will introduce the basics of CoverMe, the challenges with decrypting messages sent in this app and the measures taken to decrypt these messages.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating how to decrypt messages sent in third-party private messaging apps, specifically CoverMe, to help investigators expand their investigations and develop new techniques in their investigative process.

The increasing number of third-party private messaging apps has allowed users to send messages through the use of encryption without the worry of someone else being able to see the messages they are sending. One private messaging app in particular claiming to have "military-grade encryption" is CoverMe. CoverMe allows users to send messages at different security levels, along with the ability to remotely delete, recall messages, and set messages to self-destruct. The app also offers many other features such as private calling, private phone numbers, and a private vault. Users also have the option to set up decoy passwords along with disguising the CoverMe app to appear as a news reader app. An additional security feature of the app is that with each login attempt, it takes a picture to capture who is logging in and alerts the owner of the account.[1-3]

The security of this application and others like it may lure users to use these applications to conduct criminal activity due to these apps claiming their encryption to be "crack-proof" and very difficult for law enforcement and others to recover the artifacts relating to the investigation.[3]

A recent case presented to the laboratory presented a Samsung™ Galaxy™ S8 with suspected messages related to the crime sent and received in the CoverMe app. When extractions were performed on the phone, they appeared to be unsuccessful in decrypting the CoverMe messages. A case study was performed to determine if there was a method that allowed CoverMe messages to be decrypted that would allow the messages on the evidence phone to be recovered.

Using two Samsung™ Galaxy™ tablets, test messages were created in the CoverMe app. A physical extraction and file system extraction were performed and analyzed to determine what the CoverMe messages looked like. The messages appeared to be encrypted, and the contents of the messages were unable to be determined. The tool was able to show the login attempts along with the captured login images. Following the extractions, a secondary tool was used to see if their statement of being able to decrypt CoverMe messages held true. The physical extraction and file system extraction were uploaded into the secondary tool. The file system extraction appeared to look similar in the secondary tool as it did in the original extraction; the messages still appeared encrypted. The physical extraction when uploaded to the secondary tool was able to decrypt the messages at all security levels along with identifying the user they were being sent to and if they were incoming or outgoing. CoverMe messages sent at various security levels can be decrypted, though a physical extraction is required due to it being able to obtain a bit-by-bit copy of the phone, including hidden or deleted content.

Knowing CoverMe messages can be decrypted, the behavior of the app was then studied to aid in determining the Application Programming Interfaces (APIs) the app is calling. Studying the calls allowed for the determination of where the encryption key was being pulled from. Obtaining the encryption key CoverMe uses aids in understanding how CoverMe and other third-party messaging apps are encrypting their data.

Reference(s):

1. Botha, J., C. Van't Wout, and L. Leenen. *A Comparison of Chat Applications in Terms of Security and Privacy.* n.d. https://www.researchgate.net/publication/334537058_A_Comparison_of_Chat_Applications_in_Terms_of_Security_and_Privacy.
2. *CoverMe FAQs* [Internet]. CoverMe. [cited 12AD]; available from: http://www.coverme.ws/en/faq.html.
3. Zhang, Xiaolu, Ibrahim Baggili, and Frank Breitinger. Breaking into the Vault: Privacy, Security and Forensic Analysis of Android Vault Applications. *Computers & Security* 70 (2017): 516–31. https://doi.org/10.1016/j.cose.2017.07.011.

CoverMe, Decryption, Mobile Device Forensics

*Presenting Author